数理解析研究所講究録
458巻 1982年 94-102

非対称通信路における符号について

岩手大学工学部　大川　知

1. まえがき

最近のデータ通信の増加，計算機システムの発展にともなって，誤り検出，訂正機能をもつ符号系が一層重要になっている。以前から種々の符号が考察されているが，それらは主に対称通信路で用いることを想定したものである。しかし，ある種の装置においては，誤りに方向性があること，すなわち0が1に変ることはあっても，逆はないことが指摘されている[1]。本報告では，このような非対称通信路における符号に関するいくつかの問題を論じる。はじめに，通信路の特性のグラフ表現を与え，それを用いて通信路における誤り訂正符号を定式化する。また，符号間の距離に対応するグラフ上の距離を新たに定義する。一般のグラフ上で最大の誤り訂正符号を求める問題がNP完全であることを示す。最後に，A＝{0，1}なるアルファベットで，簡単な通信路の特性をも

つ通信路用の長さnの等長符号について検討する。

2. 準備

一般に通信路の特性は，文字aを送信したとき，文字bを受信する確率$p(a \to b)$で表現される。これを，有向グラフ$G=(A, X)$で表現する。ここで，Aはアルファベット，$X=\{(a, b) \mid p(a \to b) \neq 0\}$とする。

〔例1〕 確率pが次のように表わされているときのグラフGを図1に示す。(pは枝に付す)

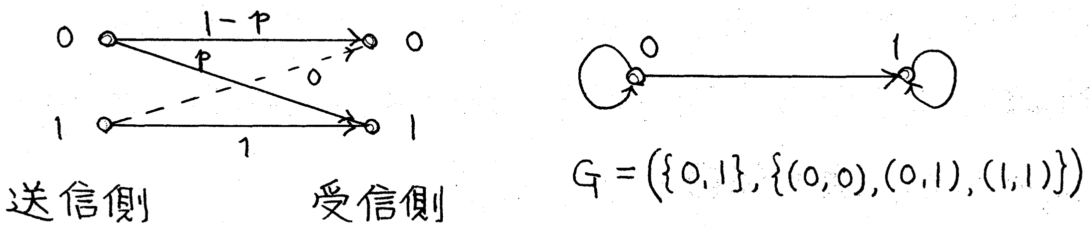
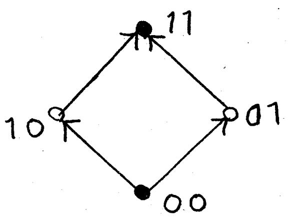


図1. 通信路の特性とそれのグラフ表現

例1の通信路において，$C=\{00, 11\}$は，誤り訂正符号となるが，$C'=\{01, 10\}$は，誤り検出符号ではあるが，訂正符号ではない。この様子は図2を見ればあきらかである。



弧は1誤りによる語の変化を示す。
00から1誤りでは，10，01のいずれかにしか到達しない。

図2. 誤り訂正符号の説明図（•はCの元）

このように，非対称的な通信路においては，符号長の短い誤り訂正符号を得る可能性がある。本報告では，$a, b \in A$

に対して $(a \neq b)$, $p(a \to b) \neq 0 \Rightarrow p(b \to a) = 0$ であるような通信路における符号を考える。

アルファベットを $A = \{a_1, a_2, \cdots, a_m\}$ とする。$p(a_i \to a_j) \neq 0$ $(i \neq j)$ のとき $(a_i, a_j) \in X$ として得られる有向グラフ $G = (A, X)$ を通信路の特性グラフという。A上の長さ n の語（信号）に対する特性を $G_n = (A^n, X_n)$ で表わす。ここで，$A^n = \{w \mid w = a_{i_1} a_{i_2} \cdots a_{i_n},\ a_{i_j} \in A\}$, $X_n = \{(w_1, w_2) \mid w_i = a_{i_1} a_{i_2} \cdots a_{i_n}\ (i = 1, 2)$ に対して，$\exists j\ (a_{1j}, a_{2j}) \in X$, かつ $\forall k\ (\neq j)\ a_{1k} = a_{2k}\}$ である。X_n はある語から，この通信路で生じうる1誤りで変る語に行く弧の集合である。

このとき，次の問題を考える。

〔問題P1〕　通信路の特性グラフ $G = (A, X)$ が与えられたとき，長さ n の1誤り訂正可能な最大の符号を求めよ。

有向グラフ $G = (N, X)$ の2点 $u, v \in N$ の間の距離 $d(u, v)$ を次のように定義する。u, v から到達可能な点の集合を $R(u)$, $R(v)$ とするとき，$d(u, v) = \min[\{l(p_{u \to v}), l(p_{v \to u})\} \cup \{l(p_{u \to w}), l(p_{v \to w}) \mid w \in R(u) \cap R(v)\}]$ とする。ここで，$p_{u \to w}$ は u から w への（単純）有向道，$l(p)$ は，道 p の長さを表わす。

〔定義1〕(2) 有向グラフ $G = (N, X)$ の点の部分集合 S が l-安全（l-safe）であるとは，$\forall x, y \in S\ (x \neq y)$ に対して，

$d(x,y) \geqq l+1$ であるときである。そのようなSのうちで元の個数が最大のものを，最大l-安全集合といい，その個数をl-安全数といい，$\sigma_l(G)$と表わす。

図2のグラフにおいて，$C=\{00, 11\}$は1-安全であり，それが最大1-安全集合であることは，あきらかであろう。

〔問題P2-l〕　有向グラフ$G=(N, X)$が与えられたとき，Gのl-安全数$\sigma_l(G)$を求めよ。

〔問題P3-l〕　有向グラフ$G=(N, X)$と正整数kが与えられたとき，Gに大きさkのl-安全集合が存在するかどうかを判定せよ。

問題P1とP2-l，P3-lの関連はあきらかであろう。また，l-安全という語は，$l=1$のとき単に安全という。

3．NP完全性

本節では，問題P3-lがNP完全であることを示す。

〔定理1〕(2) 問題P3はNP完全である。

（略証）　NP完全問題である安定集合問題が，P3に多項式時間で変換可能であることを示す。

$G=(V, E)$，$k(>0)$を安定集合問題への入力とする。このとき，$G'=(V \cup E, A_1 \cup A_2)$，$k$をP3への入力とする。ここで，$A_1=\{(u, e) \mid u \in V,\ e=\{u, v\} \in E\}$，$A_2=\{(e_1, e_2) \mid e_1, e_2 \in E,\ e_1 \cap e_2 \neq \phi\}$とする。このとき，次

の命題が成立し，多項式時間で変換可能であることが示された（証明の詳細は，文献(2)を参照のこと）。

〔系1〕 $d^+ \leq 4$，$d^- \leq 6$ なる平面グラフに対する問題P3はNP完全である。

（略証） 安定集合問題が $d \leq 3$ なる平面グラフに対してNP完全である(3)ことと，定理の証明の変換が平面性を損わないことからあきらかである。

〔系2〕 問題P3-l はNP完全である。

4. 2元完全非対称通信路における符号

前節で，問題P3がNP完全であることが示されたので，本節では，簡単な通信路の場合について考察する。すなわち2元完全非対称通信路（例1）を考える。通信路の特性グラフは $G = (\{0,1\}, \{(0,1)\})$ である。このとき，G_n $(n \geq 1)$ は束とみなすことができ，G_n の2点 u, v 間の距離は，

$$d(u, v) = \#_1(lub(u, v)) - max\{\#_1(u), \#_1(v)\}$$

である。ここで，$\#_1(u)$ は u 中の1の個数，$lub(u, v)$ は，u と v の最小上界である。

π を1から n の数の置換の集合 Π_n の任意の元とする。$u = a_{i_1} a_{i_2} \cdots a_{i_n}$ とするとき，$\pi(u) = a_{i_{\pi(1)}} a_{i_{\pi(2)}} \cdots a_{i_{\pi(n)}}$ と表わす。このとき，次の命題はあきらかである。

〔命題1〕 $d(u, v) = d(\pi(u), \pi(v))$ である。

〔補題1〕 $d(u, v) = d(\bar{u}, \bar{v})$，ここで，$\bar{u}$ は u の各桁について，0と1を反転させた語である。

（証明） 命題1より，u，v を $\alpha 0^i 1^j$，$\alpha 1^i 0^j$（$i \geqq j$）として一般性を失わない。$\bar{u}$，$\bar{v}$ はそれぞれ，$\bar{\alpha} 1^i 0^j$，$\bar{\alpha} 0^i 1^j$ であるから，$d(\bar{u}, \bar{v}) = d(u, v)$（$= i$）となる。

〔系3〕 S が G_n の安全集合ならば，$\bar{S} = \{\bar{u} \mid u \in S\}$ も G_n の安全集合である。

（証明） 補題より，$\forall\, \bar{u}, \bar{v} \in \bar{S}$ に対して，$d(\bar{u}, \bar{v}) = d(u, v)$ となり，定義よりあきらかである。

〔命題2〕 $\sigma(G_1) = 1$，$\sigma(G_2) = 2$，$\sigma(G_3) = 2$ である。

〔補題2〕 $\sigma(G_{n+2}) \geqq 2\sigma(G_n)$ である。

（略証） G_n の最大安全集合を $S_n = \{v_i \mid 1 \leq i \leq \sigma(G_n)\}$ とする。$S_{n+2} = \{v_i 00,\ v_i 11 \mid v_i \in S_n\}$ は，G_{n+2} の安全集合であり，$|S_{n+2}| = 2 \cdot \sigma(G_n)$ であるからあきらか。

〔系4〕 $\sigma(G_n) \geqq 2^{[\frac{n}{2}]}$ である。

〔補題3〕 S を，$0^n \notin S$（$1^n \notin S$）なる G_n の安全集合とする。このとき，$0^n \in S'$（$1^n \in S'$）かつ $|S'| \geqq |S|$ なる G_n の安全集合 S' が存在する。

（証明） $S^{(i)} = \{v \mid \#_1(v) = i,\ v \in S\}$ とする。$|S^{(1)}| = 0$ ならば，$S' = S \cup \{0^n\}$ とすればよいから，$S^{(1)} \neq \phi$ とする。あきらかに，$|S^{(1)}| = 1$ であるから，$S^{(1)} = \{v_1\}$ とする。

このとき，$S' = (S - \{v_1\}) \cup \{0^n\}$ とすると，$S - \{v_1\}$ は安全であり，$v \in S - S_1$ に対して，$d(0^n, v) \geqq d(v_1, v) \geqq 2$ である。よって，S' は安全である。

補題3から，最大安全集合は，0^n，1^n を含むものだけを考えればよいことがわかる。

［命題3］　$\sigma(G_4) = 4$ である。

（証明）　G_4 の最大安全集合を S_4 とする。系3より，$|S_4| \geqq 2^{\frac{4}{2}} = 4$ であるから，$|S_4| \leqq 4$ を示す。補題3より，0^n，$1^n \in S_4$ であるから，それ以外に S_4 の元としてとり得るものは，$V = \{v \mid \#_1(v) = 2\}$ の元である。任意の $v \in V$ を S_4 の元としたとき，$V - \{v' \mid d(v, v') \leqq 1\}$ の元の個数は，${}_4C_2 - \{{}_2C_1 \times {}_2C_1 + 1\} = 1$ である。よって，V からは，たかだか2元しか S_4 の元をとることができない。

［命題4］　$\sigma(G_5) = 6$ である。

（証明）　G_5 の最大安全集合を S_5 とし，0^5，$1^5 \in S_5$ とする。$d(0^5, v) \geqq 2$，$d(1^5, v) \geqq 2$ なる元は，$V_i = \{v \mid \#_1(v) = i\}$ $i = 2, 3$ の元である。$v \in V_2$ に対して，$d(v, v') \geqq 2$ なる $v' \in V_2$ の元の個数は，${}_5C_2 - ({}_3C_1 \times {}_2C_1 + 1) = 3$ である。この3個の元の間の距離はすべて1であるから，v 以外に S_5 の元としてとることのできるのは，丁度1個である。V_3 についても同様であるから，$|S_5| \leqq 1 + 2 + 2 + 1 = 6$ とな

る。実際，$S_5=\{0^5, 1^20^3, 0^21^20, (10)^21, (01)^21, 1^5\}$を選ぶことができる。よって，$\sigma(G_5)=6$である。

［命題5］　$\sigma(G_6)=12$である。

（略証）　命題4と同様にして，最大安全集合$S_6=\{0^6, (10^2)^2, (010)^2, (0^21)^2, 1^30^3, (01)^3, 0^21^30, 10^31, (01^2)^2, (101)^2, (1^20)^2, 1^6\}$が得られる。よって，$\sigma(G_6)=12$である。

以上の結果をまとめると，2元完全非対称通信路における1誤り訂正符号の大きさは次の通りである。

表1．誤り訂正符号の大きさ

語長　n	2	3	4	5	6
大きさ$\sigma(G_n)$	2	2	4	6	12

さらに，そのような符号の1つをC_nとすると，

$C_2=\{0^2, 1^2\}$，　　　$C_3=\{0^3, 1^3\}$

$C_4=\{0^4, 1^20^2, 0^21^2, 1^4\}$

$C_5=\{0^5, 1^20^3, 0^21^20, (10)^21, (01)^21, 1^5\}$（命題4）

$C_6=\{0^6, (10^2)^2, (010)^2, (0^21)^2, 1^30^3, (01)^3, 0^21^30, 10^31, (01^2)^2, (101)^2, (1^20)^2, 1^6\}$（命題5）

である。

5．むすび

本報告では，非対称通信路における最適な符号を求める問題を，グラフの安全集合を求める問題と結びつけて考察し，

それが一般的にはNP完全となることを示した。また，グラフに新しい距離を導入し，それを用いて，安全集合を l-安全集合という形に一般化し，1誤り訂正だけではなく，l 誤り訂正符号の考察を可能にした。最後に，2元完全非対称通信路におけるいくつかの最大誤り訂正符号を求めた。

熱心に討論して下さった本学情報機器学講座の皆様に感謝いたします。

文献

（1）. 鹿股，高橋，樋口：相補論理に基づく制御用マイクロコンピュータシステムの高速化，情報理論とその応用研究会資料（G－1），pp.248－253（昭56－12）.
（2）. 大川：有向グラフのある点の部分集合について（安全集合），情報処理学会第23回全国大会（3K－6），pp.21－22（昭56－10）.
（3） Garey, Johnson : Computers and Intractability,（1979）.